2. Scan web apps like a pro – vulnerability sleuth mode activated!

The Nmap Scripting Engine `NSE` is a powerful feature of the Nmap network scanning tool, designed to automate various tasks, including vulnerability detection.
`NSE` scripts can identify weaknesses in network services, web applications, and configurations by leveraging a vast library of community-contributed scripts.

In this task, you'll elevate your Nmap skills by using an NSE script to detect vulnerabilities in web applications.

Write `a bash script` that performs the following tasks:

- Your script should accept `a host` as an arguments `$1`.
- Use the `http-vuln-cve2017-5638 NSE` script to check for the Apache Struts 2 vulnerability.
- Save the output to `vuln_scan_results.txt` for later analysis.

Depending on the scanned network, the output could change.

```
┌──(maroua)-[~/0x07nmappostportscan_scripting]
└─⚑  sudo ./2-vuln_scan.sh scanme.nmap.org
[sudo] password for maroua:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-06-24 13:50 CET
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.19s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite



Nmap done: 1 IP address (1 host up) scanned in 12.19 seconds
```

The command:

```
nmap --script=http-vuln-cve2017-5638 $1 -oN vuln_scan_results.txt
```

Explanation:

1. **`nmap`**:
   - Runs the Nmap network scanner.
2. **`--script=http-vuln-cve2017-5638`**:
   - This option tells Nmap to use the **`http-vuln-cve2017-5638`** script, which is specifically designed to check if a target is vulnerable to the **CVE-2017-5638** vulnerability.
   - CVE-2017-5638 is a **Remote Code Execution (RCE)** vulnerability in Apache Struts, particularly in how the `Content-Type` header is handled by the `ActionMapper` class in Struts versions 2.3.5 to 2.3.31 and 2.5 to 2.5.10.
   - This vulnerability allows attackers to execute arbitrary commands on the server, and it was widely exploited in attacks.
3. **`$1`**:
   - A **Bash positional parameter**, which represents the **target** of the scan (IP address, hostname, or network).
   - When the script is run, you provide the target as an argument, like:

     ```
     ./yourscript.sh 192.168.1.1
     ```

   - In this case, `$1` would be replaced by `192.168.1.1`.
4. **`-oN vuln_scan_results.txt`**:
   - Directs Nmap to output the results of the scan to a file in **normal output format** (`.txt`).
   - The file will be named `vuln_scan_results.txt`, and it will contain the detailed results of the vulnerability scan for easy review later.

How It Works:

- Nmap will scan the specified target (`$1`), using the `http-vuln-cve2017-5638` script to check for the **CVE-2017-5638** vulnerability.
- The scan will focus on identifying the vulnerability in Apache Struts installations and will output the results to a file called `vuln_scan_results.txt`.

Example Usage:

If you want to scan a target with IP `192.168.1.10`, run the script as:

```
./yourscript.sh 192.168.1.10
```

This would perform the scan and save the results to `vuln_scan_results.txt`.

Sample Output (saved in `vuln_scan_results.txt`):

```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-28 15:00 UTC
Nmap scan report for 192.168.1.10
Host is up (0.0010s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-vuln-cve2017-5638:
|   VULNERABLE:
|   Apache Struts CVE-2017-5638 Remote Code Execution
|     State: VULNERABLE
|     Exploitability: High
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638
|       https://nvd.nist.gov/vuln/detail/CVE-2017-5638
|
|_  Affected versions: Apache Struts 2.3.5 to 2.3.31, 2.5 to 2.5.10

Nmap done: 1 IP address (1 host up) scanned in 5.32 seconds
```

Benefits of This Command:

1. **Targeted Vulnerability Scan**: This scan specifically targets **CVE-2017-5638**, which is a known vulnerability in Apache Struts, saving time when assessing if a server is vulnerable.
2. **Automated Output**: Storing results in a text file (`vuln_scan_results.txt`) makes it easier to track vulnerabilities and share findings.
3. **Security Posture**: Quickly checks if a system is vulnerable to a high-profile vulnerability that has been exploited in attacks.

Limitations:

1. **False Positives**: The script may sometimes report false positives if the application is misidentified as vulnerable.
2. **Limited Scope**: This script only checks for **CVE-2017-5638**, so it won't detect other vulnerabilities or configurations on the system.

Improvement Suggestions:

To scan for more vulnerabilities or apply additional checks, you can combine scripts or use other categories:

```
nmap --script=vuln,http-vuln-cve2017-5638 $1 -oN vuln_scan_results.txt
```

This command runs additional vulnerability scripts in conjunction with the **CVE-2017-5638** script.